Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - Apple iTunes Arbitrary Code Execution
  - FTGate Denial of Service or Arbitrary Code Execution
  - freeFTPd Denial of Service
  - Google Talk Denial Of Service
  - Kerio WinRoute Firewall Security Restriction Bypassing
  - Macromedia Breeze Communication Server Denial of Service
  - Macromedia Contribute Publishing Server Information disclosure
  - **Microsoft DirectX DirectShow Arbitrary Code Execution (Updated)**
  - **Microsoft Internet Explorer Arbitrary Code Execution (Updated)**
  - **Microsoft Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service (Updated)**
  - Multiple Vendor Arbitrary Code Execution
  - RealPlayer Enterprise Arbitrary Code Execution
  - StoneGate Firewall and VPN Engine Denial of Service
  - Walla! TeleSite SQL Injection or Cross-Site Scripting
- UNIX / Linux Operating Systems
  - **Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass (Updated)**
  - **Bzip2 Remote Denial of Service (Updated)**
  - **BZip2 File Permission Modification (Updated)**
  - **Linux-FTPD-SSL FTP Server Remote Buffer Overflow (Updated)**
  - Cyphor SQL Injection
  - **Eric Raymond Fetchmail POP3 Client Buffer Overflow (Updated)**
  - **Eric Raymond Fetchmail 'fetchmailconf' Information Disclosure (Updated)**
  - **FreeBSD Kernel 'sendfile()' Information Disclosure (Updated)**
  - **GNU CPIO CHMod File Permission Modification (Updated)**
  - GNU Mailman Attachment Scrubber UTF8 Filename Remote Denial of Service
  - **GNU CPIO Archiver Insecure File Creation (Updated)**
  - **Gzip Zgrep Arbitrary Command Execution (Updated)**
  - HP-UX XTerm Unauthorized Access
  - IBM AIX 'diagela' Script
  - IPCop Backup Key Information Disclosure & Race Condition
  - PNMToPNG Remote Buffer Overflow
  - **LM_sensors PWMConfig Insecure Temporary File Creation (Updated)**
  - Mike Neuman OSH Remote Buffer Overflow
  - GTK+ GdkPixbuf XPM Image Rendering Library
  - **Multiple Vendors OpenSSL Insecure Protocol Negotiation (Updated)**
  - **Multiple Vendors libungif GIF File Handling (Updated)**
  - Multiple Vendors SpamAssassin Spam Detection Bypass
  - Openswan IKE Message Remote Denials of Service
  - PADL Software MigrationTools Insecure Temporary File Creation
  - **PCRE Regular Expression Heap Overflow (Updated)**
  - Pearl Forums SQL Injection & File Inclusion
  - Peel SQL Injection
  - **PHP Apache 2 Denial of Service (Update)**
  - Redhat Sysreport Insecure Temporary File Creation
  - **Squid FTP Server Response Handling Remote Denial of Service (Updated)**
  - Sun Solaris LibIKE IKE Exchange Remote Denial of Service
  - Sun Solaris in.named Remote Denial of Service
  - **Sylpheed LDIF Import Buffer Overflow (Updated)**
  - **Todd Miller Sudo Local Elevated Privileges (Updated)**
  - Todd Miller Sudo Security Bypass
  - **Uim Elevated Privileges (Updated)**
- Multiple Operating Systems
  - **AbiWord Stack-Based Buffer Overflows (Updated)**
  - ActiveCampaign 1-2-All SQL Injection
  - AlstraSoft Template Seller Pro File Inclusion & SQL Injection
  - Antharia OnContent // CMS SQL Injection
  - Antville Cross-Site Scripting
  - **Apache HTTP Request Smuggling Vulnerability (Updated)**
  - AudienceView Cross-Site Scripting

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an

intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Apple iTunes 5.0	A vulnerability has been reported in iTunes that could let local malicious users execute arbitrary code. Upgrade to version 6.0: http://www.apple.com/itunes/download/iTunesSetup.exe There is no exploit code required.	Apple iTunes Arbitrary Code Execution	High	Security Focus, ID: 15446, November 15, 2005
Floosietek FTGate 4.0	A buffer overflow vulnerability has been reported in FTGate that could let remote malicious users cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	FTGate Denial of Service or Arbitrary Code Execution CVE-2005-3640	High	Security Focus, ID: 15449, November 16, 2005
freeFTPd 1.0.8	A vulnerability has been reported in freeFTPd that could let remote malicious users cause a Denial of Service. Upgrade to version 1.0.9: http://freeftpd.com/?ctt=download A Proof of Concept exploit has been published.	freeFTPd Denial of Service	Low	Security Tracker Alert ID: 1015230, November 16, 2005
Google Talk prior to 1.0.0.76	A vulnerability has been reported in Google Talk that could let remote malicious users cause a Denial of Service. Upgrade to version 1.0.0.76 via automatic updates. There is no exploit code required.	Google Talk Denial Of Service	Low	Security Focus, ID: 15369, November 9, 2005
Kerio WinRoute Firewall prior to 6.1.3	A vulnerability has been reported in WinRoute Firewall that could let remote malicious users bypass security restrictions. Specifically, formerly authenticated users may be able to authenticate with disabled accounts. Upgrade to version 6.1.3: http://www.kerio.com/kwf_download.html There is no exploit code required.	Kerio WinRoute Firewall Security Restriction Bypassing	Medium	Security Tracker, Alert ID: 1015194, November 11, 2005
Macromedia Breeze Communication Server 4.0, 4.1, 5.0, 5.1	A vulnerability has been reported in Breeze Communication Server that could let remote malicious users cause a Denial of Service. A vendor solution is available: http://www.macromedia.com/support/breeze/licensed_support.html#item-2 Currently we are not aware of any exploits for this vulnerability.	Macromedia Breeze Communication Server Denial of Service	Low	Macromedia, Security Bulletin MPSB05-10, November 15, 2005
Macromedia Contribute Publishing Server prior to 1.0, 1.11	A vulnerability has been reported in Contribute Publishing Server that could let remote malicious users to obtain sensitive information. Specifically, the server may utilize a weak password encryption method. A vendor update is available: http://www.macromedia.com/support/cps/downloads.html	Macromedia Contribute Publishing Server Information disclosure	Medium	Macromedia, Security Bulletin MPSB05-08, November 15, 2005

	Currently we are not aware of any exploits for this vulnerability.			
Microsoft DirectX DirectShow 7.0 to 9.0c	A buffer overflow vulnerability has been reported in DirectX DirectShow that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf **Nortel:** **http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=366955&RenditionID=** V1.3 Updated to note availability of Microsoft Knowledge Base Article 909596 and to clarify an issue affecting Windows 2000 SP4 customers, also updates of file versions. V1.4 Updated to note complications of the DirectX 8.1 update on machines running DirectX 9. Currently we are not aware of any exploits for this vulnerability.	Microsoft DirectX DirectShow Arbitrary Code Execution CVE-2005-2128	High	Microsoft, Security Bulletin MS05-050, October 11, 2005 USCERT, VU#995220 Technical Cyber Security Alert TA05-284A, October 11, 2005 Avaya, ASA-2005-214, October 11, 2005 Microsoft, Security Bulletin MS05-050 V1.3, October 21, 2005 Microsoft, Security Bulletin MS05-050 V1.4, November 9, 2005 **Nortel, Security Advisory Bulletin 2005006315, November 11, 2005**
Microsoft Internet Explorer 5.01, 5.5, 6.0	A vulnerability has been reported in Internet Explorer that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-052.mspx Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf **Nortel:** **http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=366837&RenditionID=** An exploit has been published.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2005-2127	High	Microsoft, Security Bulletin MS05-052, October 11, 2005 Technical Cyber Security Alert TA05-284A, October 11, 2005 Avaya, ASA-2005-214, October 11, 2005 USCERT, VU#680526, VU#959049, VU#740372, October 13, 2005 **Nortel, Security Advisory Bulletin 2005006317, November 11, 2005**
Microsoft Windows Microsoft Distribution Transaction Coordinator (MSDTC) and COM+	A buffer overflow vulnerability has been reported in Windows MSDTC and COM+ that could let local or remote malicious users execute arbitrary code, obtain elevated privileges or cause a Denial of Service. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-051.mspx Vendor has identified potential issues associated with fix: http://www.microsoft.com/technet/security/advisory/909444.mspx Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf **Nortel:** **http://www130.nortelnetworks.com/**	Microsoft Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service CVE-2005-1978 CVE-2005-1979 CVE-2005-1980 CVE-2005-2119	High	Microsoft, Security Bulletin MS05-051, October 11, 2005 US-CERT VU#180868, US-CERT VU#950516 Technical Cyber Security Alert TA05-284A, October 11, 2005 Microsoft, Security Advisory 909444, October 14, 2005 Avaya, ASA-2005-214, October 11, 2005 **Nortel, Security Advisory Bulletin 2005006316, November 11, 2005**

	cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=366956&RenditionID= Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors VMWare Workstation 5.0.0, RealPlayer 10.5, Microsoft AntiSpyware 1.0.509, Kaspersky Labs Anti-Virus for Windows File Servers 5.0	A vulnerability has been reported in multiple vendors software that could let local malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Multiple Vendor Arbitrary Code Execution CVE-2005-2937 CVE-2005-2936 CVE-2005-2939 CVE-2005-2940	High	Security Focus, ID: 15448, November 16, 2005
RealPlayer Enterprise 1.1, 1.2, 1.5 - 1.7	A buffer overflow vulnerability has been reported in RealPlayer Enterprise that could let remote malicious users execute arbitrary code. A vendor solution is available: http://www.service.real.com/help/faq/security/security111005.html http://www.service.real.com/help/faq/security/051110_player/EN/ Currently we are not aware of any exploits for this vulnerability.	RealPlayer Enterprise Arbitrary Code Execution CVE-2005-2629 CVE-2005-2630	High	RealNetworks, Security Patch Update For Realplayer Enterprise, November 10, 2005
Stonesoft StoneGate Firewall and VPN Engine	A vulnerability has been reported in StoneGate Firewall and VPN Engine that could let remote malicious users cause a Denial of Service. Update to newest version: https://my.stonesoft.com/download/fw https://my.stonesoft.com/download/vpn A Proof of Concept exploit has been published.	StoneGate Firewall and VPN Engine Denial of Service	Low	Stonesoft, Security Advisory IKE Vulnerabilities in StoneGate Firewall, November 14, 2005
Walla! Communications TeleSite prior to version 3.0	An input validation vulnerability has been reported in TeleSite that could let remote malicious users perform SQL injection or conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.; however a Proof of Concept exploit has been published.	Walla! TeleSite SQL Injection or Cross-Site Scripting CVE-2005-3576 CVE-2005-3577 CVE-2005-3578 CVE-2005-3579	Medium	Security Tracker Alert ID: 1015204, November 14, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Apache Software Foundation Apache 2.0.x	A vulnerability has been reported in 'modules/ssl/ssl_engine_kernel.c' because the 'ssl_hook_Access()' function does not properly enforce the 'SSLVerifyClient require' directive in a per-location context if a virtual host is configured with the 'SSLVerifyCLient optional' directive, which could let a remote malicious user bypass security policies. Patch available at: http://svn.apache.org/viewcvs?rev=264800&view=rev OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/	Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass CVE-2005-2700	Medium	Security Tracker Alert ID: 1014833, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.017, September 3, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005

errata/RHSA-2005-608.html

Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/

SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/

Debian: http://security.debian.org/pool/updates/main/a/apache2/

Mandriva: http://www.mandriva.com/security/advisories

Slackware: ftp://ftp.slackware.com/pub/slackware/

Trustix: http://http.trustix.org/pub/trustix/updates/

Debian: http://security.debian.org/pool/updates/main/liba/

Gentoo: http://security.gentoo.org/glsa/glsa-200509-12.xml

Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf

Conectiva: ftp://atualizacoes.conectiva.com.br/10/

TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/

HP: http://software.hp.com/

Trustix: http://http.trustix.org/pub/trustix/updates/

RedHat: http://rhn.redhat.com/errata/RHSA-2005-816.html

FedoraLegacy: http://download.fedoralegacy.org/

There is no exploit code required.

Debian Security Advisory, DSA 805-1, September 8, 2005

Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005

Slackware Security Advisory, SSA:2005-251-02, September 9, 2005

Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005

Debian Security Advisory DSA 807-1, September 12, 2005

US-CERT VU#744929

Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005

Avaya Security Advisory, ASA-2005-204, September 23, 2005

Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005

Turbolinux Security Advisory, TLSA-2005-94, October 3, 2005

HP Security Bulletin, HPSBUX-01232, October 5, 2005

Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005

RedHat Security Advisory, RHSA-2005:816-10, November 2, 2005

Fedora Legacy Update Advisory, FLSA:166941, November 9, 2005

bzip2 bzip2 1.0.2	A remote Denial of Service vulnerability has been reported when processing malformed archives. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.008-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-474.html FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:14/bzip2.patch Conectiva: ftp://atualizacoes.conectiva. com.br/ Debian: http://security.debian.org/pool/updates/main/b/bzip2/ SGI: http://www.sgi.com/support/security/ IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id=35093&release_id=351848 **FedoraLegacy:** **http://download.fedoralegacy.org/** Currently we are not aware of any exploits for this vulnerability.	bzip2 Remote Denial of Service CVE-2005-1260	Low	Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-60, June 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:015, June 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:14, June 29, 2005 Conectiva Linux Announce-ment, CLSA-2005:972, July 6, 2005 Debian Security Advisory, DSA 741-1, July 7, 2005 SGI Security Advisory, 20050605-01-U, July 12, 2005 Security Focus, Bugtraq ID: 13657, August 26, 2005 **Fedora Legacy Update Advisory, FLSA:158801, November 14, 2005**
bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/b/bzip2/ TurboLinux:	BZip2 File Permission Modification CVE-2005-0953	Medium	Security Focus, 12954, March 31, 2005 Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 Debian Security Advisory, DSA 730-1, May 27, 2005 Turbolinux

	ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.008-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-474.html FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:14/bzip2.patch Conectiva: ftp://atualizacoes.conectiva.com.br/ SGI: http://www.sgi.com/support/security/ **FedoraLegacy:** **http://download.fedoralegacy.org/** There is no exploit code required.			Security Advisory, TLSA-2005-60, June 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:14, June 29, 2005 Conectiva Linux Announce-ment, CLSA-2005:972, July 6, 2005 SGI Security Advisory, 20050605-01-U, July 12, 2005 **Fedora Legacy Update Advisory, FLSA:158801, November 14, 2005**
Christoph Martin linux-ftpd-ssl 0.17	A buffer overflow vulnerability has been reported in the 'vsprintf()' function in the FTP server, which could let a remote malicious user execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200511-11.xml** **Debian:** **http://security.debian.org/pool/updates/main/l/linux-ftpd-ssl/** An exploit script has been published.	Linux-FTPD-SSL FTP Server Remote Buffer Overflow CVE-2005-3524	High	Secunia Advisory: SA17465, November 8, 2005 **Gentoo Linux Security Advisory, GLSA 200511-11, November 14, 2005** **Debian Security Advisory, DSA 896-1, November 15, 2005**
Cyphor Cyphor 0.19	An SQL injection vulnerability has ben reported in 'show.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. An exploit script has been published.	Cyphor SQL Injection CVE-2005-3575	Medium	Security Focus, Bugtraq ID: 15418, November 15, 2005

Eric Raymond Fetchmail 6.2.5	A remote buffer overflow vulnerability has been reported in the POP3 client due to insufficient boundary checks, which could let a malicious user obtain elevated privileges. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Redhat: http://rhn.redhat.com/errata/RHSA-2005-640.html Ubuntu: http://www.ubuntulinux.org/support/ documentation/usn/usn-153-1 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200507-21.xml Debian: http://security.debian.org/pool/updates/main/f/fetchmail/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Fetchmail POP3 Client Buffer Overflow CVE-2005-2335	Medium	Fedora Update Notifications, FEDORA-2005-613 & 614, July 21, 2005 Redhat Security Advisory, RHSA-2005:640-08, July 25, 2005 Ubuntu Security Notice, USN-153-1, July 26, 2005 Gentoo Security Advisory, GLSA 200507-21, July 25, 2005 Debian Security Advisory, DSA 774-1, August 12, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Turbolinux Security Advisory, TLSA-2005-84, August 18, 2005 Conectiva Linux Announce-ment, CLSA-2005:1005, September 13, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:209, November 10, 2005**
Eric S Raymond Fetchmail 6.x	A vulnerability has been reported in the 'fetchmailconf' configuration utility due to a race condition, which could let a malicious user obtain sensitive information. Upgrades available at: http://download.berlios.de/fetchmail/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-06.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/f/fetchmail/ **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	Fetchmail 'fetchmailconf' Information Disclosure CVE-2005-3088	Medium	fetchmail-SA-2005-02 Security Announcement, October 21, 2005 Gentoo Linux Security Advisory, GLSA 200511-06, November 6, 2005 Ubuntu Security Notice, USN-215-1, November 07, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:209, November 10, 2005**

FreeBSD FreeBSD 5.4 & prior	A vulnerability has been reported in the 'sendfile()' system call due to a failure to secure sensitive memory before distributing it over the network, which could let a malicious user obtain sensitive information. Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:02/ **A Proof of Concept exploit script has been published.**	FreeBSD Kernel 'sendfile()' Information Disclosure CVE-2005-0708	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:02, April 5, 2005 US-CERT VU#604846 **Security Focus, Bugtraq ID: 12993, November 10, 2005**
GNU cpio 1.0-1.3, 2.4.2, 2.5, 2.5.90, 2.6	A vulnerability has been reported when an archive is extracted into a world or group writeable directory because non-atomic procedures are used, which could let a malicious user modify file permissions. Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-378.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32 Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-191.pdf Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cpio/ Debian: http://security.debian.org/pool/updates/main/c/cpio/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-806.html** There is no exploit code required.	CPIO CHMod File Permission Modification CVE-2005-1111	Medium	Bugtraq, 395703, April 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005:116, July 12, 2005 RedHat Security Advisory, RHSA-2005:378-17, July 21, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 SCO Security Advisory, SCOSA-2005.32, August 18, 2005 Avaya Security Advisory, ASA-2005-191, September 6, 2005 Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005 Ubuntu Security Notice, USN-189-1, September 29, 2005 Debian Security Advisory, DSA 846-1, October 7, 2005 **RedHat Security Advisory, RHSA-2005:806-8, November 10, 2005**
GNU Mailman 2.1-2.1.5, 2.0-2.0.14	A remote Denial of Service vulnerability has been reported in 'Scrubber.py' due to a failure to handle exception conditions when Python fails to process an email file attachment that contains utf8 characters in its filename. No workaround or patch available at time of publishing. There is no exploit code required.	GNU Mailman Attachment Scrubber UTF8 Filename Remote Denial of Service CVE-2005-3573	Low	Secunia Advisory: SA17511, November 14, 2005

GNU cpio 1.0, 1.1, 1.2	A vulnerability has been reported in 'cpio/main.c' due to a failure to create files securely, which could let a malicious user obtain sensitive information. Upgrades available at: http://ftp.gnu.org/gnu/cpio/cpio-2.6.tar.gz SGI: ftp://oss.sgi.com/projects/sgi propack/download/3/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-806.html** There is no exploit required.	CPIO Archiver Insecure File Creation CVE-1999-1572	Medium	Security Tracker Alert, 1013041, January 30, 2005 SGI Security Advisory, 20050204-01-U, March 7, 2005 Turbolinux Security Advisory, TLSA-2005-30, March 10, 2005 Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005 **RedHat Security Advisory, RHSA-2005:806-8, November 10, 2005**
GNU zgrep 1.2.4	A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands. A patch for 'zgrep.in' is available in the following bug report: http://bugs.gentoo.org/show_bug.cgi?id=90626 Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-474.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ SGI: http://www.sgi.com/support/security/ F5: http://tech.f5.com/home/bigip/solutions/advisories/sol4532.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/	Gzip Zgrep Arbitrary Command Execution CVE-2005-0758	High	Security Tracker Alert, 1013928, May 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Fedora Update Notification, FEDORA-2005-471, June 27, 2005 SGI Security Advisory, 20050605-01-U, July 12, 2005 Secunia Advisory: SA16159, July 21, 2005 Ubuntu Security Notice, USN-158-1, August 01, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Avaya Security Advisory, ASA-2005-172, August 29, 2005

	main/g/gzip/ Trustix: ftp://ftp.trustix.org0 /pub/trustix/updates/ Avaya: http://support.avaya. com/elmodocs2/ security/ASA- 2005-172.pdf **FedoraLegacy:** **http://download.** **fedoralegacy.org/** There is no exploit code required.			**Fedora Legacy Update Advisory, FLSA:158801, November 14, 2005**
Hewlett Packard Company HP-UX B.11.23, B.11.11, B.11.00	A vulnerability has been reported in HP UX running xterm, which could let a malicious user obtain unauthorized access. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	HP-UX XTerm Unauthorized Access	Medium	HP Security Advisory, HPSBUX02075, November 14, 2005
IBM AIX 5.3 L, 5.3, 5.2.2, 5.2 L, 5.2	A vulnerability has been reported in the '/usr/lpp/diagnostics/ bin/diagela.sh' script due to the use of absolute path. The impact was not specified. Updates available at: http://www-1.ibm.com/ servers/eserver/support/ pseries/aixfixes.html Currently we are not aware of any exploits for this vulnerability.	AIX 'diagela' Script	Not Specified	IBM Security Advisory, November 11, 2005
IPCop IPCop 1.4.9, 1.4.8, 1.4.6, 1.4.5, 1.4.4, 1.4.2, 1.4.1	Several vulnerabilities have been reported: a vulnerability was reported due to the way the application stores the key to encrypted backup files, which could let a malicious user obtain sensitive information; and a vulnerability was reported due to a race condition when the application changes the ownership on the file before it is encrypted, which could let a malicious user decrypt backup files. Upgrades available at: http://prdownloads. sourceforge.net/ ipcop/ipcop-sources -1.4.10.tgz?down load There is no exploit code required.	IPCop Backup Key Information Disclosure & Race Condition	Medium	Security Focus, Bugtraq ID: 15377 & 15378, November 10, 2005
libpng pnmtopng 2.38, 2.37.3-2.37.6	A buffer overflow vulnerability has been reported in 'Alphas_Of _Color' due to insufficient bounds checking of user-supplied data prior to copying it to an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads. sourceforge.net/ png-mng/pnmtopng- 2.39.tar.gz?download Currently we are not aware of any exploits for this vulnerability.	PNMToPNG Remote Buffer Overflow	High	Security Focus, Bugtraq ID: 15427, November 15, 2005

lm_sensors lm_sensors 2.9.1	A vulnerability has been reported in the 'pwmconfig' script due to the insecure creation of temporary files, which could result in a loss of data or a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lm-sensors/ Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200508-19.xml Debian: http://security.debian.org/pool/updates/main/l/lm-sensors/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-825.html** There is no exploit code required.	LM_sensors PWMConfig Insecure Temporary File Creation CVE-2005-2672	Low	Security Focus, Bugtraq ID: 14624, August 22, 2005 Ubuntu Security Notice, USN-172-1, August 23, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:149, August 25, 2005 Gentoo Linux Security Advisory, GLSA 200508-19, August 30, 2005 Debian Security Advisory, DSA 814-1, September 15, 2005 Conectiva Linux Announcement, CLSA-2005:1012, September 23, 2005 Fedora Update Notifications, FEDORA-2005-1053 & 1054, November 7, 2005 **RedHat Security Advisory, RHSA-2005:825-13, November 10, 2005**
Mike Neuman osh 1.7	A buffer overflow vulnerability has been reported in 'main.c' due to an error when handling environment variable substitutions, which could let a remote malicious user execute arbitrary with superuser privileges. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit script has been published.	Mike Neuman OSH Remote Buffer Overflow CVE-2005-3346	High	Secunia Advisory: SA17527, November 9, 2005
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; TouchTunes Rhapsody, TouchTunes Maestro; SuSE UnitedLinux 1.0, Novell Linux Desktop 9.0, Linux Professional 10.0 OSS, 10.0, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Personal 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Enterprise Server 9, 8, Linux Desktop 1.0; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, 2.1 IA64, 2.1, AS 4, AS 3, AS 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; GTK+ 2.8.6, 2.6.4, 2.4.14, 2.4.13, 2.4.10, 2.4.9, 2.4.1, 2.2.4, 2.2.3; GNOME GdkPixbuf 0.22; Gentoo Linux ; Ardour 0.99	Multiple vulnerabilities have been reported: an integer overflow vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' due to the insufficient validation of the 'n_col' value before using to allocate memory, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' when processing an XPM file that contains a large number of colors; and an integer overflow vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' when performing calculations using the height, width, and colors of a XPM file, which could let a remote malicious user execute arbitrary code or cause a Denial of Service. Updates available at: ftp://ftp.gtk.org/pub/gtk/v2.8/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-810.html Gentoo: http://security.gentoo.org/glsa/glsa-	GTK+ GdkPixbuf XPM Image Rendering Library CVE-2005-2975 CVE-2005-2976 CVE-2005-3186	High	Fedora Update Notifications FEDORA-2005-1085 & 1086, November 15, 2005 RedHat Security Advisory, RHSA-2005:810-9, November 15, 2005 Gentoo Linux Security Advisory GLSA 200511-14, November 16, 2005 SUSE Security Announcement, SUSE-SA:2005:065, November 16, 2005 Ubuntu Security Notice, USN-216-1, November 16, 2005

200511-14.xml

SuSE:
ftp://ftp.suse.com/
pub/suse/

Ubuntu:
http://security.ubuntu.
com/ubuntu/pool/
main/g/gdk-pixbuf/

Currently we are not aware of any exploits for these vulnerabilities.

Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, 2.1, IA64, ES 4, ES 3, 2.1, IA64, AS 4, AS 3, AS 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; OpenSSL Project OpenSSL 0.9.3-0.9.8, 0.9.2b, 0.9.1 c; FreeBSD 6.0 -STABLE, -RELEASE, 5.4 -RELENG, -RELEASE, 5.3 -STABLE, -RELENG, -RELEASE, 5.3, 5.2.1 -RELEASE, -RELENG, 5.2 -RELEASE, 5.2, 5.1 -RELENG, -RELEASE/Alpha, 5.1 -RELEASE-p5, -RELEASE, 5.1, 5.0 -RELENG, 5.0, 4.11 -STABLE, -RELENG, 4.10 -RELENG, -RELEASE, 4.10	A vulnerability has been reported due to the implementation of the 'SSL_OP_MSIE_SSLV2_RSA_PADDING' option that maintains compatibility with third party software, which could let a remote malicious user bypass security. OpenSSL: http://www.openssl.org/source/openssl-0.9.7h.tar.gz FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:21/openssl.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-800.html Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200510-11.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101974-1 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/openssl/ OpenPKG: ftp://ftp.openpkg.org/release/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: http://www.sgi.com/support/security/ Debian: http://security.debian.org/pool/updates/main/o/openssl094/ NetBSD: http://arkiv.netbsd.se/?ml=netbsd-announce&a=2005-10&m=1435804 BlueCoat Systems: http://www.bluecoat.com/support/knowledge/advisory_openssl_	Multiple Vendors OpenSSL Insecure Protocol Negotiation CVE-2005-2969	Medium	OpenSSL Security Advisory, October 11, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:21, October 11, 2005 RedHat Security Advisory, RHSA-2005:800-8, October 11, 2005 Mandriva Security Advisory, MDKSA-2005:179, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-11, October 12, 2005 Slackware Security Advisory, SSA:2005-286-01, October 13, 2005 Fedora Update Notifications, FEDORA-2005-985 & 986, October 13, 2005 Sun(sm) Alert Notification Sun Alert ID: 101974, October 14, 2005 Ubuntu Security Notice, USN-204-1, October 14, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.022, October 17, 2005 SUSE Security Announcement, SUSE-SA:2005:061, October 19, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 SGI Security Advisory, 20051003-01-U, October 26, 2005 Debian Security Advisory DSA 875-1, October 27, 2005 NetBSD Security Update, November 1, 2005 BlueCoat Systems Advisory, November 3, 2005 Debian Security Advisory, DSA 888-1, November 7, 2005 **Astaro Security Linux Announce-ment, November 9, 2005** **SCO Security Advisory, SCOSA-2005.48, November 15, 2005**

	\2005-2969.html Debian: http://security.debian.org/pool/updates/main/o/openssl/ **Astaro Security Linux:** **http://www.astaro.org/showflat.php?Cat=&Number=63500&page=0&view=collapsed&sb=5&o=&fpart=1#63500** **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.48** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, WS 2.1, IA64, ES 4, ES 3, ES 2.1, IA64, AS 4, AS 3, 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; libungif libungif 4.1.3, 4.1, giflib 4.1.3; Gentoo Linux	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported due to a NULL pointer dereferencing error; and a vulnerability was reported due to a boundary error that causes an out-of-bounds memory access, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=102202 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-03.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-828.html SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libu/libungif4/ Debian: http://security.debian.org/pool/updates/main/libu/libungif4/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors libungif GIF File Handling CVE-2005-2974 CVE-2005-3350	High	Security Tracker Alert ID: 1015149, November 3, 2005 Fedora Update Notifications, FEDORA-2005-1045 & 1046, November 3, 2005 Gentoo Linux Security Advisory GLSA 200511-03, November 4, 2005 RedHat Security Advisory, RHSA-2005:828-17, November 3, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Ubuntu Security Notice, USN-214-1, November 07, 2005 Debian Security Advisory, DSA 890-1, November 9, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:207, November 10, 2005**
Multiple Vendors SpamAssassin 3.0.4; RedHat Fedora Core3	A vulnerability has been reported due to a failure to handle exceptional conditions, which could let a remote malicious user bypass spam detection. SpamAssassin: http://spamassassin.apache.org/downloads.cgi?update=200509141634 Fedora: http://download.fedora.	SpamAssassin Spam Detection Bypass CVE-2005-3351	Medium	Fedora Update Notification, FEDORA-2005-1065, November 9, 2005

	redhat.com/pub/fedora/linux/core/updates/3/ There is no exploit code required.			
Openswan Openswan 2.2-2.4, 2.1.4-2.1.6, 2.1.2, 2.1.1	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported when handling IKE packets that have an invalid 3DES key length; and a remote Denial of Service vulnerability was reported when handling certain specially crafted IKE packets. Upgrades available at: http://www.openswan.org/download/openswan-2.4.2.tar.gz Vulnerabilities can be reproduced using the PROTOS ISAKMP Test Suite.	Openswan IKE Message Remote Denials of Service	Low	CERT-FI & NISCC Joint Vulnerability Advisory, November 15, 2005
PADL Software Pty Ltd MigrationTools 46	A vulnerability has been reported due to the insecure creation of 'nis.$$.ldif' temporary files, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	PADL Software MigrationTools Insecure Temporary File Creation	Medium	Secunia Advisory: SA17530, November 15, 2005

PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-17.xml Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Debian: http://security.debian.org/pool/updates/main/p/pcre3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.1/testing/packages/php-5.0.5/php-5.0.5-i486-1.tgz Gentoo: http://security.gentoo.org/glsa/glsa-200509-08.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-12.xml Debian: http://security.debian.org/pool/updates/main/p/python2.2/ Gentoo: http://security.gentoo.org/glsa/glsa-	PCRE Regular Expression Heap Overflow CVE-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices, USN-173-1 & 173-2, August 24, 2005 Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005 SUSE Security Announcements, SUSE-SA:2005:048 & 049, August 30, 2005 Slackware Security Advisories, SSA:2005-242-01 & 242-02, August 31, 2005 Ubuntu Security Notices, USN-173-3, 173-4 August 30 & 31, 2005 Debian Security Advisory, DSA 800-1, September 2, 2005 SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005 Slackware Security Advisory, SSA:2005-251-04, September 9, 2005 Gentoo Linux Security Advisory, GLSA 200509-08, September 12, 2005 Conectiva Linux Announce-ment, CLSA-2005:1009, September 13, 2005 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Debian Security Advisory, DSA 817-1 & DSA 819-1, September 22 & 23, 2005 Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005 Debian Security Advisory, DSA 821-1, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005

	200509-19.xml Debian: http://security.debian.org/pool/updates/main/p/python2.3/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-216.pdf Trustix: http://http.trustix.org/pub/trustix/updates/ **HP:** **http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE** Currently we are not aware of any exploits for this vulnerability.			Turbolinux Security Advisory, TLSA-2005-92, October 3, 2005 Avaya Security Advisory, ASA-2005-216, October 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 **HP Security Bulletin, HPSBUX02074, November 16, 2005**
Pearl Forums Pearl Forums 2.0	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'forumsId' and 'topicId' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'index.php' due to insufficient verification of the 'mode' parameter before used to include files, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Pearl Forums SQL Injection & File Inclusion	Medium	Secunia Advisory: SA17533, November 15, 2005
PEEL PEEL 2.7, 2.6	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'rubid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Peel SQL Injection CVE-2005-3572	Medium	Secunia Advisory: SA17536, November 14, 2005
PHP PHP 5.0 .0-5.0.5, 4.4 .0, 4.3.1 -4.3.11, 4.2-4.2.3, 4.1.0-4.1.2, 4.0 0-4.0.7	A Denial of Service vulnerability has been reported in the 'sapi_apache2.c' file. PHP 5.1.0 final and 4.4.1 final are not affected by this issue. Please contact the vendor to obtain fixes. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200511-08.xml** There is no exploit code required.	PHP Apache 2 Denial of Service CVE-2005-3319	Low	Security Focus, Bugtraq ID: 15177, October 24, 2005 **Gentoo Linux Security Advisory, GLSA 200511-08, November 14, 2005**

RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, 2.1, ES 4, ES 3, 2.1, AS 4, AS 3, 2.1, Advanced Workstation for the Itanium Processor 2.1	A vulnerability has been reported in sysreport due to the insecure creation of temporary files, which could let a malicious user obtain sensitive information. RedHat: http://rhn.redhat.com/errata/RHSA-2005-598.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ There is no exploit code required.	Redhat Sysreport Insecure Temporary File Creation CVE-2005-2104	Medium	Fedora Update Notifications FEDORA-2005-1071 & 1072, November 10, 2005
Squid Squid 2.x	A remote Denial of Service vulnerability has been reported when handling certain FTP server responses. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE11-rfc1738_do_escape.patch Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.44 SUSE: ftp://ftp.suse.com/pub/suse/ **IPCop:** **http://prdownloads.sourceforge.net/ipcop/ipcop-sources-1.4.10.tgz?down load** There is no exploit code required.	Squid FTP Server Response Handling Remote Denial of Service CVE-2005-3258	Low	Secunia Advisory: SA17271, October 20, 2005 Fedora Update Notifications, FEDORA-2005-1009 & 1010, October 20, 2005 Mandriva Linux Security Advisory, MDKSA-2005:195, October 26, 2005 SCO Security Advisory, SCOSA-2005.44, November 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 **Security Focus, Bugtraq ID: 15157, November 10, 2005**
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0, 9.0 _x86, 9.0	A remote Denial of Service vulnerability has been reported due to an error in the 'libike' library when processing IKE messages. Patches available at: http://sunsolve.sun.com/tpatches Vulnerability can be reproduced using the PROTOS ISAKMP Test Suite.	Sun Solaris LibIKE IKE Exchange Remote Denial of Service	Low	Sun(sm) Alert Notification Sun Alert ID: 102040, November 14, 2005
Sun Microsystems, Inc. Solaris 9.0 _x86 Update 2, 9.0 _x86, 9.0	A remote Denial of Service vulnerability has been reported in 'in.named' when multiple requests are submitted to the DNS server Patches available at: http://sunsolve.sun.com There is no exploit code required.	Sun Solaris in.named Remote Denial of Service	Low	Sun(sm) Alert Notification, 102030, November 8, 2005
Sylpheed Sylpheed 2.0-2.0.3, 1.0.0-1.0.5	A buffer overflow vulnerability has been reported in 'ldif.c' due to a boundary error in the 'ldif_get_line()' function when importing a LDIF file into the address book, which could let a remote malicious user obtain unauthorized access. Upgrades available at: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.6.tar.gz	Sylpheed LDIF Import Buffer Overflow CVE-2005-3354	Medium	Bugtraq ID: 15363, November 9, 2005 **Fedora Update Notification, FEDORA-2005-1063, November 9, 2005** **Gentoo Linux Security Advisory, GLSA 200511-13, November 15, 2005**

	Fedora: **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200511-13.xml** Currently we are not aware of any exploits for this vulnerability.			
Todd Miller Sudo 1.x	A vulnerability has been reported in the environment cleaning due to insufficient sanitization, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/s/sudo/ Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sudo/ SUSE: ftp://ftp.suse.com/pub/suse/ **An exploit script has been published.**	Todd Miller Sudo Local Elevated Privileges CVE-2005-2959	Medium	Debian Security Advisory, DSA 870-1, October 25, 2005 Mandriva Linux Security Advisory, MDKSA-2005:201, October 27, 2005 Ubuntu Security Notice, USN-213-1, October 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 **Security Focus, Bugtraq ID: 15191, November 10, 2005**
Todd Miller Sudo prior to 1.6.8p12	A vulnerability has been reported due to an error when handling the 'PERLLIB,' 'PERL5LIB,' and 'PERL5OPT' environment variables when tainting is ignored, which could let a malicious user bypass security restrictions and include arbitrary library files. Upgrades available at: http://www.sudo.ws/sudo/download.html There is no exploit code required; however, a Proof of Concept exploit script has been published.	Todd Miller Sudo Security Bypass	Medium	Security Focus, Bugtraq ID: 15394, November 11, 2005
Uim Uim 0.5 .0, 0.4.9	A vulnerability has been reported in 'uim/uim-custom.c' due to the incorrect use of several environment variables, which could let a malicious user obtain elevated privileges. Updates available at: http://uim.freedesktop.org/releases/uim-0.4.9.1.tar.gz Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/u/uim/** There is no exploit code required.	Uim Elevated Privileges CVE-2005-3149	Medium	Secunia Advisory: SA17043, October 4, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:198, October 26, 2005 **Debian Security Advisory, DSA 895-1, November 14, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source

Abi Source Community AbiWord 2.2.0-2.2.10, 2.2.12, 2.0.1-2.0.9	Multiple stack-based buffer overflow vulnerabilities have been reported due to insufficient bounds checking of user-supplied data prior to copying it to an insufficiently sized memory buffer while importing RTF files, which could let a remote malicious user execute arbitrary code. The vendor has addressed this issue in AbiWord version 2.2.11. Users are advised to contact the vendor to obtain the appropriate update. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/abiword/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200510-17.xml **Debian:** **http://security.debian.org/pool/updates/main/a/abiword/** Currently we are not aware of any exploits for these vulnerabilities.	AbiWord Stack-Based Buffer Overflows CVE-2005-2972	High	Ubuntu Security Notice, USN-203-1, October 13, 2005 Fedora Update Notification, FEDORA-2005-989, October 13, 2005 Conectiva Linux Announcement, CLSA-2005:1035, October 14, 2005 Gentoo Linux Security Advisory, GLSA 200510-17, October 20, 2005 **Debian Security Advisory, DSA 894-1, November 14, 2005**
Active Campaign ActiveCampaign 1-2-All Broadcast Email 4.0 7	An SQL injection vulnerability has been reported in the Admin Control Panel Username due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ActiveCampaign 1-2-All SQL Injection	Medium	Security Focus Bugtraq ID: 15400, November 12, 2005
AlstraSoft Template Seller Pro 3.25	Several vulnerabilities have been reported: a vulnerability was reported in 'include/paymentplugins/payment_paypal.php' due to insufficient verification of the 'config[basepath]' parameter before used to include files, which could let a remote malicious user execute arbitrary code; and an SQL injection vulnerability was reported in the administration interface due to insufficient sanitization of the username field when logging in, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AlstraSoft Template Seller Pro File Inclusion & SQL Injection	High	Secunia Advisory: SA17603, November 16, 2005
Antharia OnContent // CMS	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'pid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Antharia OnContent // CMS SQL Injection	Medium	Secunia Advisory: SA17596, November 16, 2005
Antville Antville 1.1	A Cross-Site Scripting vulnerability has been reported in 'notfound.skin' due to insufficient sanitization of the query string, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Antville Cross-Site Scripting CVE-2005-3530	Medium	Security Focus, Bugtraq ID: 15372, November 9,2005
Apache	A vulnerability has been reported in Apache which can be exploited by remote malicious users to smuggle http requests. Conectiva: http://distro.conectiva.com.br/ atualizacoes/index.php?	Apache HTTP Request Smuggling Vulnerability CVE-2005-1268 CVE-2005-2088	Medium	Secunia, Advisory: SA14530, July 26, 2005 Conectiva, CLSA-2005:982, July 25, 2005 Fedora Update Notification

	id=a&anuncio=000982 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/a/apache/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ IBM has released fixes for Hardware Management Console addressing this issue. Users should contact IBM for further information. Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ **HP:** **http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE** Currently we are not aware of any exploits for this vulnerability.			FEDORA-2005-638 & 639, August 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:129, August 3, 2005 Ubuntu Security Notice, USN-160-1, August 04, 2005 Turbolinux Security Advisory, TLSA-2005-81, August 9, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 SUSE Security Announcement, SUSE-SA:2005:046, August 16, 2005 Debian Security Advisory DSA 803-1, September 8, 2005 Ubuntu Security Notice, USN-160-2, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Security Focus, Bugtraq ID: 14106, September 21, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 Slackware Security Advisory, SSA:2005-310-04, November 7, 2005 **HP Security Bulletin, HPSBUX02074, November 16, 2005**
Audience View Software Corporation AudienceView	A Cross-Site Scripting vulnerability has been reported in 'error.asp' due to insufficient sanitization of the 'TSerrorMessage' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	AudienceView Cross-Site Scripting	Medium	Secunia Advisory: SA17582, November 16, 2005
BASE Basic Analysis and Security Engine BASE Basic Analysis and Security Engine 1.2	An SQL injection vulnerability has been reported in 'base_qry_main.php' due to insufficient sanitization of the 'sig[1] parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. **Debian:** **http://security.debian.org/pool/updates/main/a/acidlab/** There is no exploit code required; however, a Proof of Concept exploit has been published.	Basic Analysis and Security Engine SQL Injection CVE-2005-3325	Medium	Secunia Advisory: SA17314, October 25, 2005 **Debian Security Advisory DSA 893-1, November 14, 2005**

Belkin F5D7232-4, F5D7230-4	A vulnerability has been reported in the router's web-based management page due to an access control error, which could let a malicious user bypass security restrictions. No workaround or patch available at time of publishing. There is no exploit code required.	Belkin Wireless Routers Remote Authentication Bypass	Medium	Secunia Advisory: SA17601, November 16, 2005
Cisco Systems Adaptive Security Applicance 7.0 (4), 7.0 (2), 7.0 (0)	A remote Denial of Service vulnerability has been reported due to insufficient validation of ARP responses. No workaround or patch available at time of publishing. There is no exploit code required.	Cisco Adaptive Security Applicance Remote Denial of Service	Low	Security Focus, Bugtraq ID: 15407, November 14, 2005
Cisco Systems Cisco 7920 Wireless IP Phone 1.0 (8)	Several vulnerabilities have been reported: a vulnerability was reported in the SNMP service with fixed community strings that could allow remote malicious users to read, write, and erase the configuration of an affected device; and a vulnerability was reported in an open VxWorks Remote Debugger on UDP port 17185 that may allow an unauthenticated remote malicious user to access debugging information or cause a Denial of Service. Update information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051116-7920.shtml There is no exploit code required.	Cisco 7920 Wireless IP Phone Fixed SNMP Community String & Open UDP Port	Medium	Cisco Security Advisory, cisco-sa-20051116-7920, November 16, 2005
Cisco Systems Firewall Services Module (FWSM) 1.x, 2.x, IOS 12.x, IOS R12.x, PIX 4.x, 5.x, 6.x, 7.x, Cisco SAN-OS 1.x (MDS 9000 Switches), 2.x (MDS 9000 Switches), VPN 3000 Concentrator	A remote Denial of Service vulnerability has been reported due to errors in the processing of IKEv1 Phase 1 protocol exchange messages. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec.shtml Vulnerability can be reproduced with the PROTOS IPSec Test Suite.	Cisco IPSec IKE Traffic Remote Denial of Service	Low	Cisco Security Advisory, Document ID: 68158, November 14, 2005
CodeGrrl PHPQuotes 1.0; PHPFanBase 2.1; PHPClique 1.0; PHPCalendar 0.10.3	A vulnerability has been reported in 'protection.php' due to insufficient verification of the 'siteurl' parameter before used to include files, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	CodeGrrl Products File Inclusion CVE-2005-3571	High	Secunia Advisory: SA17542, November 14, 2005
contentServ contentServ 3.1	A vulnerability has been reported in 'admin/about.php' due to insufficient verification of the 'ctsWebsite' parameter before including files, which could let a remote malicious user include arbitrary files. **The vendor has released a Hotfix to address this issue. This fix is available for registered customers from the vendor Website.** An exploit script has been published.	ContentServ Local File Include CVE-2005-3086	Medium	Security Focus, Bugtraq ID: 14943, September 26, 2005 **Security Focus Bugtraq ID: 14943, November 10, 2005**
Dev-Editor Dev-Editor 3.0, 2.3-2.3.2, 2.2 a, 2.1 a, 2.1, 2.0	A vulnerability has been reported due to the way virtual directories are handled, which could let a remote malicious user bypass security restrictions. Updates available at: http://sourceforge.net/project/showfiles.php?group_id=4197 There is no exploit code required.	Dev-Editor Security Bypass	Medium	Secunia Advisory: SA17537, November 11, 2005
EKINdesigns Ekinboard 1.0.3	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'profile.php' script due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported due to insufficient satiation of the forum Topic Title before using, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ekinboard Cross-Site Scripting & Script Injection CVE-2005-3638	Medium	Security Tracker Alert ID: 1015207, November 15, 2005

Exponent Exponent 0.96 .1	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported due to insufficient sanitization of user-supplied input in the image upload portion of the application, which could let a remote malicious user execute arbitrary script code. Upgrade available at: http://prdownloads.sourceforge.net/exponent/exponent-0.96.4.tar.gz There is no exploit code required.	Exponent CMS Multiple SQL Injection & Image Upload	High	Security Focus, Bugtraq ID: 15389 & 15391, November 11, 2005
First 4 Internet XCP-Aurora	Several unspecified vulnerabilities have been reported in the kernel driver contained in the First 4 Internet XCP-Aurora DRM software, which could let a malicious user obtain SYSTEM level privileges No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	First 4 Internet XCP-Aurora Multiple Vulnerabilities	High	Internet Security Systems Protection Alert, November 15, 2005
First4Internet CodeSupport	A vulnerability has been reported due to a failure to verify that the source of remote content is from a trusted source before downloading, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	First 4 Internet CodeSupport Remote Arbitrary Code Execution CVE-2005-3650	High	Security Focus, Bugtraq ID: 15430, November 15, 2005 US-CERT VU#312073
Francisco Burzi PHP-Nuke 7.0-7.8	An SQL injection vulnerability has been reported in the 'search' module due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPNuke SQL Injection	Medium	Security Focus, Bugtraq ID: 15421, November 15, 2005
Help Center Live Help Center Live 2.0, 1.2-1.2.8, 1.0	A file include vulnerability has been reported in 'module.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Help Center Live File Include	Medium	Security Focus, Bugtraq ID: 15404, November 14, 2005
Horde Project Horde 2.2-2.2.8	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of unspecified parameters before returning to the user in error messages, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/horde/horde-2.2.9.tar.gz There is no exploit code required.	Horde Error Message Cross-Site Scripting CVE-2005-3570	Medium	Secunia Advisory: SA17468, November 14, 2005
IBM DB2 Content Manager 8.2 Fix Pack 1-9	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the library server due to an error when creating a text index of an imported Excel file; and a remote Denial of Service vulnerability has been when handling LZH files due to an unspecified error. Update available at: http://www-1.ibm.com/support/docview.wss?uid=swg24010789 Currently we are not aware of any exploits for these vulnerabilities.	IBM DB2 Content Manager Remote Denials of Service CVE-2005-3568 CVE-2005-3569	Low	Secunia Advisory: SA17388, November 10, 2005
Juniper Networks T-series Router T320, M-series Router M5, M40e, M40, M20, M160, M10, J-series	Multiple unspecified vulnerabilities have been reported that include buffer overflows, format strings, and Denials of Service when handling malformed IKEv1 traffic. The vendor has reported addressed these issues in E Series Routers in releases 5-2-4p0-8, 5-2-5, 5-3-4p0-5,	Juniper Networks Routers ISAKMP IKE Traffic Multiple Vulnerabilities	High	CERT-FI & NISCC Joint Vulnerability Advisory, November 14, 2005

Services Router J6300, J4300, J2300, E-series Router	6-0-2p0-5, 6-0-3, 6-1-1p0-7, 6-1-2, 7-0-0p0-1, 7-0-1, and 7-1-0. M, T, and J Series Routers releases 6.4 and later address this issue in releases built on July 28, 2005 and after. Vulnerabilities can be reproduced using the PROTOS ISAKMP Test Suite.			
KDE KDE 3.4, 3.3-3.3.2, 3.2-3.2.3	A vulnerability has been reported in KDE Kate and KWrite because backup files are created with default permissions even if the original file had more restrictive permissions set, which could let a local/remote malicious user obtain sensitive information. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-612.html Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ **Debian: http://security.debian.org/pool/updates/main/k/kdelibs/** There is no exploit code required.	KDE Kate, KWrite Local Backup File Information Disclosure CVE-2005-1920	Medium	Security Tracker Alert ID: 1014512, July 18, 2005 Fedora Update Notification, FEDORA-2005-594, July 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:122, July 20, 2005 RedHat Security Advisory, RHSA-2005:612-07, July 27, 2005 Conectiva Linux Announcement, CLSA-2005:988, August 4, 2005 Debian Security Advisory, DSA 804-1, September 8, 2005 **Debian Security Advisory, DSA 804-2, November 10, 2005**
Macromedia Flash 7.0.19 .0, 7.0 r19, 6.0.79 .0, 6.0.65 .0, 6.0.47 .0, 6.0.40 .0, 6.0.29 .0, 6.0	A vulnerability has been reported due to insufficient validation of the frame type identifier that is read from a SWF file, which could let a remote malicious user execute arbitrary code. Update information available at: http://www.macromedia.com/devnet/security/security_zone/mpsb05-07.html **Microsoft: http://www.microsoft.com/technet/security/advisory/910550.mspx** An exploit has been published.	Macromedia Flash Array Index Remote Arbitrary Code Execution CVE-2005-2628	High	Macromedia Security Advisory, MPSB05-07, November 5, 2005 **Microsoft Security Advisory (910550), November 10, 2005** **US-CERT VU#146284**
Macromedia Flash 7.0.19 .0 & prior	An input validation vulnerability has been reported in 'ActionDefine Function' due to an error for a critical array index value, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Update information available at: http://www.macromedia.com/devnet/security/security zone/mpsb05-07.html **Microsoft: http://www.microsoft.com/technet/security/advisory/910550.mspx** A Proof of Concept exploit has been published.	Macromedia Flash Input Validation CVE-2005-3591	High	Macromedia Security Bulletin, MPSB05-07, November 7, 2005 **Microsoft Security Advisory (910550), November 10, 2005**

Macromedia Flash Communication Server MX 1.5, 1.0	A remote Denial of Service vulnerability has been reported due to insufficient validation of some RTMP data. Patches available at: http://download.macromedia.com/pub/flashcom/updaters/1_0_release_3/fcs_win_updater_r3.zip Currently we are not aware of any exploits for this vulnerability.	Macromedia Flash Communication Server MX RTMP Data Validation	Low	Macromedia Security Bulletin, MPSB05-09, November 15, 2005
Mambo Mambo Site Server 4.0.14, 4.0.12 RC1-RC3, BETA & BETA 2, 4.0.10-4.0.12, 4.0	A remote file include vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary remote PHP code. No workaround or patch available at time of publishing. There is no exploit code required.	Mambo Open Source Remote File Include	High	Security Focus, Bugtraq ID: 15461, November 16, 2005
Moodle moodle 1.6 dev, 1.5-1.5.2, 1.4.1-1.4.3, 1.3- 1.3.4, 1.2-1.2.1 Moodle moodle 1.2-1.2.1, 1.1.1	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'category.php' and 'info.php' due to insufficient sanitization of the 'id' parameter, and in 'plot.php' due to insufficient sanitization of the 'user' parameter, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability has been reported in 'junpto.php' due to insufficient sanitization of the 'jump' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Moodle Cross-Site Scripting & SQL Injection CVE-2005-3648 CVE-2005-3649	Medium	Secunia Advisory: SA17526, November 11, 2005
Multiple Vendors Snort Project Snort 2.4.0-2.4.2; Nortel Networks Threat Protection System Intrusion Sensor 4.1, Nortel Networks Threat Protection System Defense Center 4.1	A buffer overflow vulnerability has been reported in the Back Orifice processor due to a failure to securely copy network-derived data into sensitive process buffers, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.snort.org/dl/current/snort-2.4.3.tar.gz Nortel: http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=SWDETAIL&SoftwareOID=362101 Exploit scripts have been published.	Snort Back Orifice Preprocessor Remote Buffer Overflow CVE-2005-3252	High	Internet Security Systems Protection Advisory, October 18, 2005 Technical Cyber Security Alert TA05-291A, October 18, 2005 **US-CERT VU#175500** Security Focus, Bugtraq ID: 15131, October 25, 2005

Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; AbiSource Community AbiWord 2.2 .0-2.2.9, 2.0.1-2.0.9	A buffer overflow vulnerability has been reported in the RTF importer due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.abisource.com/downloads/abiword/2.2.10/source/abiword-2.2.1 0.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/abiword/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-20.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Debian:** **http://security.debian.org/pool/updates/main/a/abiword/** Currently we are not aware of any exploits for this vulnerability.	AbiWord RTF File Processing Remote Buffer Overflow CVE-2005-2964	High	Security Tracker Alert ID: 1014982, September 28, 2005 Ubuntu Security Notice, USN-188-1, September 29, 2005 Fedora Update Notification, FEDORA-2005-955, September 30, 2005 Gentoo Linux Security Advisory, GLSA 200509-20, September 30, 2005 Conectiva Linux Announcement, CLSA-2005:1035, October 14, 2005 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 **Debian Security Advisory, DSA 894-1, November 14, 2005**
Multiple Vendors University of Kansas Lynx 2.8.5 & prior	A vulnerability has been reported in the 'lynxcgi:' URI handler, which could let a remote malicious user execute arbitrary commands. Upgrades available at: http://lynx.isc.org/current/lynx2.8.6dev.15.tar.gz RedHat: http://rhn.redhat.com/errata/RHSA-2005-839.html Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200511-09.xml There is no exploit code required.	Lynx URI Handlers Arbitrary Command Execution CVE-2005-2929	High	Security Tracker Alert ID: 1015195, November 11, 2005 RedHat Security Advisory, RHSA-2005:839-3, November 11, 2005 Mandriva Linux Security Advisory, MDKSA-2005:211, November 12, 2005 Gentoo Linux Security Advisory, GLSA 200511-09, November 13, 2005
Multiple Vendors Gentoo Linux; Apache Software Foundation Apache 2.1-2.1.5, 2.0.35-2.0.54, 2.0.32, 2.0.28, Beta, 2.0 a9, 2.0	A remote Denial of Service vulnerability has been reported in the HTTP 'Range' header due to an error in the byte-range filter. Patches available at: http://issues.apache.org/bugzilla/attachment.cgi?id=16102 Gentoo: http://security.gentoo.org/glsa/glsa-200508-15.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-	Apache Remote Denial of Service CVE-2005-2728	Low	Secunia Advisory: SA16559, August 25, 2005 Security Advisory, GLSA 200508-15, August 25, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 Fedora Update Notifications, FEDORA-2005-848 & 849, September 7, 2005

	608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Debian: http://security.debian.org/pool/updates/main/a/apache2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf Conectiva: ftp://atualizacoes.conectiva.com.br/10/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Trustix: http://http.trustix.org/pub/trustix/updates/ **FedoraLegacy:** **http://download.fedoralegacy.org/** **HP:** **http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE** There is no exploit code required.			Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005 Avaya Security Advisory, ASA-2005-204, September 23, 2005 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005 Turbolinux Security Advisory, TLSA-2005-94, October 3, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 **Fedora Legacy Update Advisory, FLSA:166941, November 9, 2005** **HP Security Bulletin, HPSBUX02074, November 16, 2005**
Multiple Vendors phpSysInfo 2.0-2.3	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user conduct Cross-Site Scripting attacks, phishing style attacks, and retrieve privileged or sensitive information. Upgrades available at: http://prdownloads.sourceforge.net/phpsysinfo/phpSysInfo-2.4.tar.gz?download Debian: http://security.debian.org/pool/updates/main/p/phpsysinfo/	phpSysInfo Multiple Vulnerabilities CVE-2005-3347 CVE-2005-3348 CVE-2003-0536	Medium	Hardened PHP Project Security Advisory, November 13, 2005 Debian Security Advisory, DSA 897-1, November 15, 2005

	There is no exploit code required; however, Proof of Concept exploits have been published.			
Multiple Vendors RedHat Fedora Core4, Core3; PHP 5.0.4, 4.3.9	A remote Denial of Service vulnerability has been reported when parsing EXIF image data contained in corrupt JPEG files. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-831.html** Currently we are not aware of any exploits for this vulnerability.	PHP Group Exif Module Remote Denial of Service CVE-2005-3353	Low	Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005 **RedHat Security Advisory, RHSA-2005:831-15, November 10, 2005**
Multiple Vendors Symantec AntiVirus Corporate Edition 8.0;RAV AntiVirus Desktop 8.6; Microsoft AntiSpyware beta 1; Kaspersky Labs Anti-Virus Personal 4.5.104, Anti-Virus for Windows File Servers 4.5.104; Frisk Software F-Prot Antivirus 3.16 c; ClamWin 0.87; Avast! Antivirus Professional Edition 4.6.603	A vulnerability has been reported when processing a file that contains an obscured file name, which could let malicious files bypass detection. No workaround or patch available at time of publishing. There is no exploit code required.	Multiple Vendor Antivirus Products Obscured File Name Scan Bypass	Medium	XFOCUS Security Team Advisory, xfocus-AD-051115, November 15, 2005
Multiple Vendors Ukranian National Antivirus UNA; Trend Micro PC-cillin 2005, OfficeScan Corporate Edition 7.0; Sophos Anti-Virus 3.91; Panda Titanium Norman Virus Control 5.81; McAfee Internet Security Suite 7.1.5; Kaspersky Labs Anti-Virus 5.0.372; Ikarus Ikarus 2.32; F-Prot Antivirus 3.16 c; eTrust CA 7.0.14; Dr.Web 4.32 b; AVG Anti-Virus 7.0.323; ArcaBit ArcaVir 2005.0	A vulnerability has been reported in the scanning engine routine that determines the file type if the MAGIC BYTE of the EXE files is at the beginning, which could lead to a false sense of security and arbitrary code execution. Trend Micro PC-cillin 2006 is not affected by this issue. Please contact the vendor to obtain fixes. **Kaspersky Labs states that as of 11 November, 2005, a fix is available for all affected versions of Kaspersky Labs Anti-Virus. This fix is available through the normal signature update functionality.** A Proof of Concept exploit has been published.	Multiple Vendors Anti-Virus Magic Byte Detection Evasion CVE-2005-3370 CVE-2005-3371 CVE-2005-3372 CVE-2005-3373 CVE-2005-3374 CVE-2005-3375 CVE-2005-3376 CVE-2005-3377 CVE-2005-3378 CVE-2005-3379 CVE-2005-3380 CVE-2005-3381 CVE-2005-3382 CVE-2005-3399 CVE-2005-3400 CVE-2005-3401	High	Security Focus, Bugtraq ID: 15189, October 25, 2005 Security Focus, Bugtraq ID: 15189, October 31, 2005 **Security Focus, Bugtraq ID: 15189, November 15, 2005**
MyBB Group My BulletinBoard 1.0 PR2, RC1- RC4	Several vulnerabilities have been reported: a vulnerability was reported in the subject field when a new thread is created due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in the Reputation system due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported because malicious users can delete or move other users' private messages (PM); and a remote Denial of Service vulnerability was reported due to an unspecified error. Updates available at: http://www.mybboard.net/mybb_pr2_20051101.zip There is no exploit code required.	MyBulletinBoard Multiple Vulnerabilities	Medium	Secunia Advisory: SA17577, November 15, 2005

MyBB Group MyBulletinBoard 1.0 PR2, RC4	An SQL injection vulnerability has been reported in 'Usercp.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. **Patches available at: http://community.mybboard.net/attachment.php?aid=1505** There is no exploit code required; however, a Proof of Concept exploit script has been published.	MyBulletinBoard SQL Injection CVE-2005-3326	Medium	Security Focus, Bugtraq ID: 15204, October 26, 2005 **Security Focus, Bugtraq ID: 15204, November 15, 2005**
Nortel Networks Nortel Networks Switched Firewall 6000 series, 5100 series, 5000 series, 5100	Multiple unspecified vulnerabilities have been reported in IKEv1, which could let a remote malicious user execute arbitrary code and completely compromise affected devices. Update information available at: http://www116.nortelnetworks.com/pub/repository/CLARIFY/DOCUMENT/2005/46/019857-02.pdf Currently we are not aware of any exploits for these vulnerabilities.	Nortel Switched Firewall IKE Traffic Multiple Unspecified Vulnerabilities	High	Nortel Networks Security Advisory, November 15, 2005
OcoMon OcoMon 1.21, 1.20 0, 1.11-1.14	SQL injection vulnerabilities have been reported due to insufficient sanitization of unspecified parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	OcoMon Unspecified SQL Injection	Medium	Secunia Advisory: SA17470, November 11, 2005
PHP GEN PHP GEN 1.0-1.2	Cross-Site Scripting vulnerabilities have been reported due to insufficient satiation of unspecified input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.eyce.be/php_gen/downloads/php_gen-1.3.tgz There is no exploit code required.	PHP GEN Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 15458, November 16, 2005
PHP Group PHP 5.0.5, 4.4.0	A vulnerability has been reported in the 'open_basedir' directive due to the way PHP handles it, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Trustix: http://http.trustix.org/pub/trustix/updates/ Upgrades available at: http://www.php.net/ **Gentoo: http://security.gentoo.org/glsa/glsa-200511-08.xml** There is no exploit code required.	PHP 'Open_BaseDir' Information Disclosure CVE-2005-3054	Medium	Security Focus, Bugtraq ID: 14957, September 27, 2005 Ubuntu Security Notice, USN-207-1, October 17, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 Security Focus, Bugtraq ID: 14957, October 31, 2005 **Gentoo Linux Security Advisory, GLSA 200511-08, November 13, 2005**
PHP PHP 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x, 5.0.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of the 'GLOBALS' array, which could let a remote malicious user define global variables; a vulnerability was reported in the 'parse_str()' PHP function when handling an unexpected termination, which could let a remote malicious user enable the 'register_globals' directive; a Cross-Site Scripting vulnerability was reported in the 'phpinfo()' PHP function due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an integer overflow vulnerability was reported in 'pcrelib' due to an error, which could let a remote malicious user corrupt memory. Upgrades available at: http://www.php.net/get/php-4.4.1.tar.gz	PHP Multiple Vulnerabilities CVE-2005-3388 CVE-2005-3389 CVE-2005-3390 CVE-2005-3391 CVE-2005-3392	Medium	Secunia Advisory: SA17371, October 31, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Turbolinux Security Advisory TLSA-2005-97, November 5, 2005 Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005 **RedHat Security Advisories, RHSA-2005:838-3 & RHSA-2005:831-15,**

	SUSE: ftp://ftp.suse.com /pub/suse/ TurboLinux: ftp://ftp.turbolinux.co. jp/pub/TurboLinux/ TurboLinux/ia32/ Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates/ **RedHat:** **http://rhn.redhat. com/errata/RHSA- 2005-838.html** **http://rhn.redhat. com/errata/RHSA- 2005-831.html** **Gentoo:** **http://security.gentoo. org/glsa/glsa- 200511-08.xml** There is no exploit code required.			**November 10, 2005** **Gentoo Linux Security Advisory, GLSA 200511-08, November 13, 2005**
phpAds New phpAdsNew 2.0.6	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'logout.php' due to insufficient sanitization of the 'sessionID' cookie before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'misc/revisions/ create.php' because sensitive information is disclosed when accessed directly; and a vulnerability was reported because it is possible to disclose the full path to other scripts by accessing them directly. Upgrades available at: http://prdownloads. sourceforge.net/ phpadsnew/phpAds New-2.0.7.tar.gz?download There is no exploit code required; however, a Proof of Concept exploit has been published.	phpAdsNew Information Disclosure & SQL Injection CVE-2005-3645 CVE-2005-3646	Medium	Secunia Advisory: SA17464, November 10, 2005
phpMyAdmin phpMyAdmin 2.7.0-beta1	An HTTP response splitting vulnerability has been reported in 'Header_HTTP_ Inc.php' due to insufficient sanitization of user-supplied input, which could lead to a false sense of trust. No workaround or patch available at time of publishing. There is no exploit code required.	PHPMyAdmin HTTP Response Splitting CVE-2005-3621	Medium	Fitsec Security Advisory, November 15, 2005
phpSysInfo phpSysInfo 2.3	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. It is also possible to obtain the full path to certain scripts. Debian: http://security.debian. org/pool/updates/main/ p/phpsysinfo/ **Debian:** **http://security.debian. org/pool/updates/ main/p/phpsysinfo/** There is no exploit code required; however, Proofs of Concept exploits have been published.	PHPSysInfo Multiple Cross-Site Scripting CVE-2005-0870	High	Secunia Advisory, SA14690, March 24, 2005 Debian Security Advisory, DSA 724-1, May 18, 2005 **Debian Security Advisory, DSA 897-1, November 15, 2005**
phpwcms phpwcms 1.2.5 -DEV	Several vulnerabilities have been reported: a vulnerability was reported in 'login.php' due to insufficient verification of the 'form_lang' parameter before used to include files, which could let a remote malicious user include arbitrary files; a vulnerability was reported in 'random_ image.php' due to insufficient verification of the 'imgdir' parameter before used to view a random image, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability was reported in 'act_	phpwcms File Include, Information Disclosure & Cross-Site Scripting	Medium	Secunia Advisory: SA17590, November 16, 2005

	newsletter.php' due due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.			
PhpWeb Things PhpWebThings 1.4	An SQL injection vulnerability has been reported in the 'MSG' parameter due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, an exploit script has been published.	PHPWebThings MSG Parameter SQL Injection	Medium	Security Focus, Bugtraq ID: 15465, November 16, 2005
PhpWeb Things PhpWebThings 1.4	An SQL injection vulnerability has been reported in 'download.php' due to insufficient sanitization of the 'file' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPWebThings SQL Injection	Medium	Security Focus, Bugtraq ID: 15399, November 12, 2005
Pollvote Pollvote	A vulnerability has been reported in 'pollvote.php' due to insufficient verification of the 'pollname' parameter before using to include files, which could let a remote malicious user execute arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	Pollvote File Include	High	Security Focus, Bugtraq ID: 15439, November 15, 2005
Real Networks RealOne 1, 2; RealPlayer 8, 10, 10.5	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported because a remote malicious user can create a RealMedia (.rm) movie file with a specially crafted first data packet and execute arbitrary code; a buffer overflow vulnerability was reported because a remote malicious user can create a specially crafted RealPlayer skin file (.rjs) and execute arbitrary code; and a buffer overflow vulnerability was created because a remote malicious user can create a specially crafted skin file and execute arbitrary code. Patches available at: http://www.service.real.com/help/faq/security/051110_player/EN/ Currently we are not aware of any exploits for these vulnerabilities.	RealPlayer/ RealOne Player .rm Files & Skin Files Buffer Overflows CVE-2005-2629 CVE-2005-2630	High	Security Tracker Alert ID: 1015185, November 11, 2005
Scorched 3D Scorched 3D 39.1, 37.1, 37.0, 36.0-36.2, 35.0	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported due to boundary and format string errors in various functions, which could let a remote malicious user execute arbitrary code; a vulnerability as reported in 'ServerConnect Handler.cpp' due to an error when handing the 'numplayers' field, which could let a remote malicious user freeze a vulnerable server; a buffer overflow vulnerability was reported in 'ComsMessage Handler.cpp' due to an error when creating error messages, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported in 'Logger.cpp' due to an error when handling overly large values. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200511-12.xml** A Proof of Concept exploit has been published.	Scorched 3D Multiple Vulnerabilities CVE-2005-3486 CVE-2005-3487 CVE-2005-3488	High	Secunia Advisory: SA17423, November 4, 2005 **Gentoo Linux Security Advisory, GLSA 200511-12, November 15, 2005**
Secgo Software Crypto IP Gateway 3.2.26, 3.2, 3.0.82, 3.0, 2.3, Crypto IP Client 3.2.26, 3.2, 3.1, 3.0.82, 3.0, 2.3	Multiple unspecified vulnerabilities have been reported that include buffer overflows and Denials of Service in the IKEv1 implementation. Updates available at: https://software.secgo.com Vulnerabilities can be reproduced using the PROTOS ISAKMP Test Suite.	Secgo Software Crypto IP Gateway/Client IKEv1 Traffic Multiple Vulnerabilities	High	CERT-FI & NISCC Joint Vulnerability Advisory, November 14, 2005

TikiWiki Project TikiWiki 1.8.5, 1.8.4	A Directory Traversal vulnerability has been reported in 'tiki-editpage. php' and 'Tiki-User_ Preferences.PHP' due to insufficient sanitization, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://prdownloads. sourceforge.net/ tikiwiki/tikiwiki- 1.9.1.1.tar.gz There is no exploit code required.	TikiWiki Directory Traversal CVE-2005-1925	Medium	iDefense Security Advisory, November 10, 2005
TikiWiki Project TikiWiki 1.9-1.9.2,	Several vulnerabilities have been reported: a Cross-Site vulnerability was reported in 'Tiki--view_forum_thread.php' due to insufficient sanitization of the 'topics_offset' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'tiki-view-forum_thread.php' because it can be accessed with an invalid 'topics_sort_mode' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	TikiWiki Cross-Site Scripting & Information Disclosure CVE-2005-3528 CVE-2005-3529	Medium	Secunia Advisory: SA17521, November 10, 2005
Veritas Software NetBackup Server 5.1, 5.0, NetBackup Enterprise Server 5.1, 5.0, NetBackup Client 5.1, 5.0	A buffer overflow vulnerability has been reported in a shared library used by the VERITAS NetBackup volume manager daemon (vmd), which could let a remote malicious user potentially execute arbitrary code or cause a Denial of Service. Patches available at: http://support.veritas. com/menu_ddProduct_ NBUESVR_view_ DOWNLOAD.htm Currently we are not aware of any exploits for this vulnerability.	VERITAS NetBackup Volume Manager Daemon Buffer Overflow CVE-2005-3116	High	Symantec Security Advisory, SYM05-024, November 8, 2005 **US-CERT VU#574662**
W3C Libwww 5.4	Multiple unspecified vulnerabilities have been reported including a buffer overflow and vulnerabilities related to the handling of multipart/byteranges content. The impact was not specified. Fedora: http://download.fedora. redhat.com/pub/ fedora/linux/core/ updates/ **Mandriva:** **http://www.mandriva.** **com/security/** **advisories** Currently we are not aware of any exploits for these vulnerabilities.	W3C Libwww Multiple Unspecified Vulnerabilities CVE-2005-3183	Not Specified	Fedora Update Notifications, FEDORA- 2005-952 & 953, October 7, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:210, November 10, 2005**
Wizz Forum Wizz Forum	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Wizz Forum Multiple SQL Injection	Medium	Security Focus, Bugtraq ID: 15410, November 14, 2005
Xoops Xoops 2.2.3, WF-Downloads 2.0.5	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'viewcart.php' due to insufficient sanitization of the 'list' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'class/xoops editor/textarea/editor_ registry.php' due to insufficient verification of the 'xoopsConfig[language]' parameter before used to include files, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	XOOPS Multiple Input Validation	Medium	Security Focus, Bugtraq ID: 15406, November 14, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Firms admit to mobile security shambles:** According to findings from the Mobile Usage Survey 2005, a third of professionals using mobile devices such as PDAs and smartphones admit to not using passwords or any other security protection despite three out of 10 storing their Pins, passwords and other corporate information on the devices. Source: http://www.vnunet.com/vnunet/news/2146149/mobile-security-shambles.

Wireless Vulnerabilities

- Belkin Wireless Routers Remote Authentication Bypass: A vulnerability has been reported due to a flaw in the Web administration interface authentication process.
- Cisco 7920 Wireless IP Phone Fixed SNMP Community String & Open UDP Port: Several vulnerabilities have been reported including a fixed SNMP community string vulnerability and an open UDP port vulnerability.
- aircrack-2.4.tgz: An 802.11 WEP cracking program.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
November 16, 2005	phpwebth14_xpl.php	No	Exploit for the PHPWebThings MSG Parameter SQL Injection Vulnerability.
November 16, 2005	phpwebthing-144-sql.pl	No	Proof of Concept exploit for the PHPWebThings SQL Injection vulnerability.
November 16, 2005	PNPDoS.c	No	Script that exploits the Microsoft Windows Plug and Play Denial of Service Vulnerability.
November 15, 2005	BlockingSkype-rootn0de2005.pdf	N/A	Whitepaper called Blocking Skype Using Squid And OpenBSD.
November 15, 2005	cyphor_sql.pl cyphorSQL.txt	No	Exploits for the Cyphor SQL Injection vulnerability.
November 15, 2005	EasyPageCMSXSS.txt	No	Exploit details for the EasyPageCMS Cross-Site Scripting vulnerability.
November 15, 2005	FTGate-expl.pl	No	Proof of Concept exploit for the Floosietek FTGate IMAP Server Buffer Overflow vulnerability.
November 15, 2005	iwar-0.01.tar.gz	N/A	A war dialer written for Unix type (Linux/OpenBSD/etc) operating systems that supports a nice curses based front end, ASCII/MySQL logging, system identification, multiple modems support, random/sequential dialing, key stroke logging, and more.
November 15, 2005	md4coll.c	N/A	MD4 collision generator.
November 15, 2005	md5coll.c	N/A	MD5 collision generator tool.
November 15, 2005	md5coll.zip	N/A	MD5 collision generator tool. Windows port with source.
November 15, 2005	PHPNuke-sp3x.pl	No	Proof of Concept exploit for the PHPNuke SQL Injection vulnerability.
November 15, 2005	sudo_local_perl_root.txt	Yes	Proof of Concept exploit for the Todd Miller Sudo Security Bypass vulnerability.
November 15, 2005	unb153pl3_xpl.html	No	Exploit for the Unclassified NewsBoard SQL Injection vulnerability.
November 15, 2005	upnp-dos.c	No	Denial of Service exploit that makes use of a memory leak when sending a specially crafted upnp_getdevicelist request.
November 15, 2005	walla30.txt	No	Exploitation details for the Walla! TeleSite SQL Injection or Cross Site Scripting vulnerabilities.
November 14, 2005	Wizz_Forum_SQL.pl wizzSQL.txt	No	Exploits for the Wizz Forum Multiple SQL Injection vulnerabilities.
November 13, 2005	aircrack-2.4.tgz	N/A	An 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered. It implements the standard FMS attack along with some optimizations, thus making the attack much faster compared to other WEP cracking tools.
November 13, 2005	SF_multi.pl.txt	Yes	Exploit for the VERITAS Cluster Server for UNIX Buffer Overflow vulnerability.
November 13, 2005	xoops_xpl.html XOOPS_WFd205_xpl.php	Yes	Exploit details for the Xoops XOOPS Multiple Input Validation Vulnerabilities.
November 12, 2005	ZH200502.txt	No	Exploit details for the phpAdsNew Information Disclosure & SQL Injection vulnerabilities.

November 11, 2005	SF_multi.pl	Yes	Perl script that exploits the VERITAS Cluster Server for UNIX Buffer Overflow vulnerability.
November 10, 2005	freebsd_sendfile.c	Yes	Proof of Concept exploit for the FreeBSD Kernel 'sendfile()' Information Disclosure vulnerability.
November 10, 2005	fsigk_exp.py.txt	Yes	Proof of Concept exploit for the F-Secure Anti-Virus Gatekeeper & Gateway for Linux Elevated Privileges vulnerability.
November 10, 2005	moodle16dev_xpl.php moodle16dev.txt	No	Proof of Concept exploits for the Moodle SQL Injection vulnerabilities.
November 10, 2005	sudo_local_root.txt	Yes	Script that exploits the Todd Miller Sudo Local Elevated Privileges vulnerability.
November 10, 2005	sudo168p10.sh.txt	Yes	Exploit for the Todd Miller Sudo Local Elevated Privileges vulnerability.
November 10, 2005	susechfn.sh.txt	Yes	Script that exploits the Multiple Vendors CHFN User Modification ROOT Access vulnerability.
November 10, 2005	x_osh3.sh	No	Proof of Concept exploit for the Mike Neuman OSH Environment Variable Buffer Overflow Vulnerability.

[back to top]

Trends

- **CSI: Survey shows most companies still vulnerable to attacks:** According to Qualys Inc. research, even though companies are making significant progress in their overall patching practices, nearly seven out of 10 business systems currently remain vulnerable to exploits and attacks. Source: http://www.computerworld.com/newsletter/0,4902,106244,00.html?nlid=PM.
- **Bots may get cloak of encryption:** According to a SRA International speaker at the Computer Security Institute conference, bots will include encryption to hide their presence from security and network sniffing tools often used to detect their presence. Source: http://news.com.com/Bots+may+get+cloak+of+encryption/2100-7349_3-5952102.html?tag=alert.
- **Phishing Alert: ASB Bank:** Websense® Security Labs™ has received reports of a new phishing attack that targets customers of ASB Bank. Users receive a spoofed email message, which claims that their billing information is outdated. Users are provided a link to a fraudulent website where they are prompted for Fastnet Access Code and Fastnet Password. Source: http://www.websensesecurity labs.com/alerts/alert.php?AlertID=338.
- **New IM Phishing Attack Unleashed On Yahoo:** According to the IMlogic Threat Center a new phishing attack that sends IM users a message telling them their account will be blocked unless they respond to a terms of service violation. IM.Marphish.Yahoo sends a message that appears to be from the Yahoo "abuse department" informing users that they are in violation of their agreement. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=173601765.
- **Pay up or lose out:** According to a new survey by Unisys, American consumers are so fearful of online fraud that 40 percent are willing to pay fees for additional protection. This is an increase from last year when just over a quarter of those surveyed would be willing to do the same. Source: http://www.securityfocus.com/brief/46.
- **New Sober variant hits inboxes:** Antivirus vendors have warned of a new outbreak of the Sober virus, which security firm Symantec referred to as Sober S. Source: http://www.itweek.co.uk/vnunet /news 2146131/virus-firms-warn-against-sober .
- **Keyloggers Jump 65% As Info Theft Goes Mainstream:** According to VeriSign iDefense the number of keyloggers unleashed by hackers increased by 65% this year as E-criminals rush to steal identities and information. Keyloggers are on the upswing because they make money for their handlers. Once activated, a keylogger can track and record personal data such as account numbers or passwords, or silently steal login information to later access corporate networks to hijack confidential information. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID= 173603195&tid=6004.
- **Internet Security Market To Reach $58 Billion By 2010:** According to a report from Business Communications, the global Internet security market is expected to grow at an annual rate of 16% over the next five years to reach $58.1 billion by 2010. Source: http://www.informationweek.com/story/ showArticle.jhtml?articleID=173603199&tid=6004.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.

2	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling anti virus, and modifying data.
3	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
4	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
5	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
6	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
7	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
8	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
10	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.

Table updated November 14, 2005

[back to top]

Last updated November 17, 2005